UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

JEFFREY MCBRIDE	)	**CLASS ACTION COMPLAINT**
	)	
v.	)	**CV-**
	)	
STOCKX, L.L.C.	)	
	)	
	)	
	)	
	)	

CLASS ACTION COMPLAINT

Plaintiff, through undersigned counsel, files on behalf of himself and all persons similarly situated, this Class Action Complaint, alleging the following based on personal knowledge, investigation of counsel and review of public documents. Among other things, as to allegations regarding the Plaintiff and on information and belief as to other allegations.

INTRODUCTION

1. This is a civil action seeking monetary damages, restitution and declaratory relief from Defendant StockX, L.L.C ("StockX") arising from a data breach announced to the public on August 3, 2019 ("the Data Breach").

2. Plaintiff alleges that StockX failed to secure and safeguard personal information ("Personal Information") and payment card or other financial information ("Financial Information") (collectively, "Private Information[1]"), that StockX collected and maintained, and

[1] As defined herein and used throughout this Complaint, "Private Information" includes all information exposed by the data breach, including but not limited to portions of a victim's name, address, postal code, shoe size, shopping preferences, phone numbers, email addresses, dates of birth, Social Security number, driver's license information, tax identification number, bank account number, credit card number, personal images, income, credit scores, credit limits, account balances, payment history, and transaction data.

that StockX failed to provide timely and adequate notice to Plaintiff and other Class members with details regarding what Private Information had been stolen.

3. In May of 2019, the Private Information of an unknown number of customers, believed to be approximately 6.8 million accounts, was compromised as a result of StockX's failure to adequately secure individual's Private Information on its systems.

4. An unknown third party ("hacker") took advantage of glaring weaknesses and vulnerabilities in the company's data security systems. StockX's security protocols were so deficient the breach continued for three months while StockX failed to even detect it.

5. While the hacker was the perpetrator of the breach, its occurrence was inevitable. StockX's systemic incompetence and a lackluster approach to data security has existed within the company for years and is ingrained in its culture from the top down. StockX's failure to seriously address data security persisted despite warnings by outside cybersecurity experts and other numerous, high-profile data breaches at other major American corporations, including Home Depot, Target, Michaels and Equifax, all of which should have alerted StockX's of the need to revamp and enhance its inadequate data security practices.

6. Plaintiff's Private Information was exposed by StockX. He seeks to recover damages and equitable relief on behalf of himself and all others similarly situated in the United States.

JURISDICTION AND VENUE

7. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiff alleges that StockX violated the FCRA.

8. In addition, this Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (1) the Class consists of more than 100 members; (2) the amount at

issue is more than $5 million exclusive of interest and costs; and (3) minimal diversity exists as at least one plaintiff is a citizen of a different state than Defendant.

9. This Court has jurisdiction over StockX because the company regularly conducts business in Pennsylvania and has sufficient minimum contacts in Pennsylvania and StockX, which has its principal headquarters in Michigan, has intentionally availed itself of this jurisdiction by marketing and selling products in Pennsylvania and other consumers nationwide.

10. Venue in this Court is appropriate pursuant to 28 U.S.C. § 1391(a) because a substantial part of the events, acts, or omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

11. The Plaintiff brings this action on behalf of himself and those similarly situated across the United States and within their States or Territories of residence. As with the rest of the millions of victims of the data breach, StockX through its actions described herein leaked, disbursed, or furnished Private Information to unknown cyber criminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

12. Plaintiff Jeffrey McBride is a U.S. resident and citizen of the Commonwealth of Pennsylvania, living in Philadelphia. Upon information and belief, his Private Information was compromised in the Data Breach. Before the announcement of the breach, Plaintiff was a regular customer of StockX and had bought and sold sneakers on the StockX platform on numerous occasions. Like millions of others who used Defendant's website, he created a profile through which he provided his Private Information in connection with his use of Defendant's online platform.

13. StockX failed to safeguard the privacy and security of his information. Plaintiff would not have submitted his Private Information had he known of StockX's inadequate data

security practices. Given the highly sensitive nature of the information stolen, Plaintiff remains at a substantial and imminent risk of future harm.

14. Plaintiff is one of many individuals that have been impacted by the data breach.

15. Defendant StockX LLC is a Michigan limited liability company with its principal place of business in Detroit, Michigan. StockX is in the sneaker, watch, handbag and street wear re-sale market operating the website www.StockX.com. StockX is an industry leader in gauging the market value of sneakers world-wide.

CLASS ACTION ALLEGATIONS

16. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Fed. R. Civ. P. 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance and superiority requirements of Rule 23.

17. The proposed classes are defined as:

NATIONWIDE CLASS

> All natural persons in the United States, within the applicable statute of limitations preceding the filing of this action to the date of class certification, whose Private Information was compromised as a result of the Data Breach.

18. The Nationwide Class asserts claims against StockX for violation of the FCRA (Count 1), negligence (Count 2), negligence misrepresentation (Count 3) and Violation of the Michigan Identity Theft Statute (Count 4). The Nationwide Class also requests a declaratory judgment (Count 7).

19. Excluded from the Nationwide Class is StockX and any of its parents, affiliates, or subsidiaries as well as any successors in interest or assigns of StockX, the attorneys representing the class and the Judge assigned this litigation.

20. Upon information and belief, Plaintiff is a member of the Nationwide Class, as defined above.

STATEWIDE SUBCLASS

> All natural persons and entities in the Commonwealth of Pennsylvania, within the applicable statute of limitations preceding the filing of this action to the date of class certification, whose Personal Information was compromised as a result of the Data Breach.

21. Upon information and belief, Plaintiff is a member of the Statewide Class, as defined above. The Statewide Class asserts claims against StockX for Intrusion Upon Seclusion (Count 5) and Violations of Pennsylvania's Unfair Trade Practices and Consumer Protection Law (Count 6). The Statewide Class also requests a declaratory judgment (Count 7).

22. The members of the above Classes are readily ascertainable and StockX has access to addresses and other contact information that may be used for providing notice to class members.

23. The members of the classes are so numerous that joinder of all members would be impracticable. Plaintiff is informed and believes—based in part upon StockX's press releases — that there are millions of class members in the U.S. Those individuals' names and addresses are available from StockX's records, and class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. There are also thousands of class members within each class.

24. There are substantial questions of law and fact common to the classes that predominate over questions affecting only individual Class members including, but not limited to, the following:

a. Whether StockX owed a duty to the Plaintiff and the classes to adequately protect Private Information;

b. Whether StockX breached its duty to protect Private Information by failing to provide adequate security;

c. Whether StockX knew or should have known that its computer systems were vulnerable to attack;

d. Whether StockX failed to take adequate and reasonable measures to ensure its data systems were protected;

e. Whether StockX failed to take available steps to prevent and stop the Data Breach from happening;

f. Whether StockX's conduct (or lack thereof) was the direct and proximate cause of the Data Breach of its systems, which resulted in the loss or disclosure of Private Information;

g. Whether StockX improperly retained transaction data beyond the period of time permitted by law;

h. Whether Defendant unreasonably delayed in notifying affected customers of the Data Breach and whether the belated notice was adequate;

i. Whether StockX negligently failed to inform the Plaintiff and the Class regarding the vulnerabilities of its data protection systems, measures and practices;

j. Whether StockX's conduct amounted to violations of the FCRA (15 USC §§ 1681, *et seq.*), state consumer protection statutes, and/or state data breach or privacy statutes;

k. Whether the Plaintiff and the Class suffered injury as a result of StockX's conduct (or lack thereof);

l. Whether the Plaintiff and the Class are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief; and

m. What is the appropriate measure of damages sustained by the Plaintiff and the Class?

25. Plaintiff's claims are typical of the Class. The same events and conduct that give rise to Plaintiff's claims are identical to those that give rise to the claims of every other class member because Plaintiff has suffered harm as a direct and proximate cause of the same, specific Data Breach described herein.

26. Plaintiff will fairly and adequately represent the interests of the class. Plaintiff has retained counsel who are experienced and qualified in prosecuting complex class action and data

breach litigation similar to this one and Plaintiff intends to prosecute this action vigorously. The class members' interests will be fairly and adequately protected by Plaintiff and his counsel. Neither Plaintiff nor his attorneys have any interest contrary to or conflicting with those of other members of the Class.

27. The prosecution of separate actions by individual class members seeking declaratory and injunctive relief pursuant to Rule 23(b)(2) would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for StockX. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other class members and impair their interests. StockX has acted and/or refused to act on grounds generally applicable to the class, making final injunctive relief or corresponding declaratory relief appropriate.

28. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the other class members' claims is economically unfeasible and procedurally impracticable. Litigating the claims of the class together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and unnecessary expense to the parties and the courts.

29. Even if class members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

COMMON FACTUAL ALLEGATIONS

A. What StockX Does

30. StockX is a billion-dollar company. The company earns revenue through a flat transaction fee and by taking a percentage of each sale. The website acts as a middleman, securing and safeguarding transactions between buyers and sellers that do not know each other.

31. As part of its security measures, StockX reviews and authenticates all products for sale before they are delivered. Both buyers and sellers ("users") are required to create an online profile with the company which includes sensitive and personally-identifying information, including name, email address, password, shoe size, payment information and other related profile information.

32. In addition, StockX requires users to provide payment information with a link to a payment method (for example, PayPal or a credit/debit card) when placing bids.

B. StockX Discovers the Breach and Takes Action

33. On or around August 3, 2019, TechCruch and other media outlets reported that more than 6.8 million records were stolen from StockX's website in May of 2019 by a hacker. *See* https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/?tpcc=ECTW2019 (last visited August 9, 2019). The hacker tried to sell the stolen data on the "dark web." *Id.*

34. Prior to that, StockX told users that as a result of "system updates," they should reset their customer passwords after it was "alerted to suspicious activity." 8/3/19 email sent to customers.

35. This alert to customers was not entirely true. Following the TechCruch article, StockX came clean and eventually admitted that there was a Data Breach.

36. The stolen data purportedly contained names, email addresses, user passwords, device type, and other profile information.

Plaintiff received notice from Defendant that there was an event that caused it to recommend that their "community" change passwords, but did not inform Plaintiff and other users that there was a data breach. In fact, his and other class members' Private Information stored and maintained by Defendant was put at risk.

C. StockX Understood the Value of Data Security

37. Like any merchant that handles payment cards and other sensitive data, StockX was required to maintain the security and confidentiality of Private Information and protect it from unauthorized disclosure.

38. The Payment Card Industry Data Security Standards ("PCI DSS") are a list of twelve information security requirements promulgated by the Payment Card Industry Security Standards Council. They apply to all organizations and environments where cardholder data is stored, processed, or transmitted and require organizations to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks and ensure the maintenance of information security policies. In addition, the PCI DSS prohibits StockX from retaining certain customer data. Specifically, the PCI DSS 2.0 requires merchants to adhere to the following rules:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access

- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel

39. StockX was at all times fully cognizant of its data protection obligations in light of the existing web of regulations requiring it to take affirmative steps to protect the sensitive financial information entrusted to it by consumers and the institutions that participate in and administer payment card processing systems.

40. Despite this, StockX's treatment of the sensitive Private Information entrusted to it by its customers and the Plaintiff fell woefully short of its legal duties and obligations. StockX failed to ensure that access to its data systems was reasonably guarded and protected, and failed to acknowledge numerous warning signs and properly utilize its own security systems that were put in place to detect and deter this exact type of attack.

41. At the time of the breach, StockX had specific notice of the potential threat of a data breach, and of the potential risks posed to the company and to the Plaintiff and the Class if it failed to adequately protect its systems.

42. As early as 2005, a notorious IT systems hacker, Albert Gonzalez, masterminded and implemented one of the largest coordinated data breaches in history, ultimately compromising more than 170 million credit and debit card accounts by infecting retailers' point of sale ("POS") terminals with malicious software (also known as malware) which transmitted, unencrypted, the financial data being processed by the POS machine to Gonzalez and his accomplices. In the end, Gonzalez and his cohorts were able to walk off with vast amounts of customer data from various retailers.

43. Several noteworthy reports published in 2013 put, or should have put, all businesses on notice of the increase in cyber-attacks in the U.S. For instance, Visa Corporation issued reports alerting about specific attacks. To guard against the threat, Visa instructed companies to review its "firewall configuration and ensure only allowed ports, services and IP addresses are communicating with your network"; "segregate the payment processing network from other non-payment processing networks"; "implement hardware-based point-to-point encryption"; "perform periodic scans on systems to identify storage of cardholder data and securely delete the data"; and "assign strong passwords to your security solution to prevent application modification." StockX did not implement these measures.

44. StockX's awareness of the importance of data security was bolstered in part by its observation of numerous other well-publicized data breaches involving major corporations being targeted for consumer information.

45. Through a series of data breaches extending back to 2013, more than three billion Yahoo user accounts were compromised when account holders' names, addresses, and dates of birth were stolen. The hackers also stole users' passwords, both encrypted and unencrypted, and security questions and answers.

46. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target Stores and The Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.

47. In the Summer of 2014, a data breach of JP Morgan Chase compromised the data of 76 million American households and 7 million small businesses. Breached data included

contact information (names, addresses, phone numbers, and email addresses) as well as "internal information about the users."

48. In early 2015, Anthem, the second-largest health insurer in the United States, suffered a data breach that exposed the names, addresses, Social Security numbers, dates of birth, and employment histories of nearly 80 million current and former plan members.

49. Perhaps most significantly, data breaches to credit reporting agencies Experian, in 2015, exposing more than 15 million people's information, to Equifax, the largest breach yet, exposing more than half the countries' personal and financial information, and to Capital One, almost simultaneously with StockX, exposing 100 million accounts.

50. Unfortunately, StockX did not view these breaches as cautionary tales, but rather as another avenue to profit from businesses and consumers concerned with fraud.

D. The Impact of the StockX Data Breach is Significant

51. There is no doubt that data breaches put consumers at an increased risk of fraud and identify theft. Private Information is a valuable commodity to identity thieves. Once information has been compromised, it often exists on the black-market for years.

52. As a direct and proximate result of StockX's conduct, Plaintiff and class members are at an increased risk of harm from fraud and identity theft, and have suffered or will suffer actual injury as a direct result of the Data Breach. Injuries that have and will be incurred include: fraudulent charges, loss of use of and access to their account funds and costs associated with that such as paying late or declined payment fees, damage to credit, out-of-pocket costs such as purchasing credit monitoring and identity theft prevention, the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

53. In addition, Plaintiff and class members have an interest in ensuring that their Private Information is protected from further breaches through security measures and safeguards.

54. StockX's completely avoidable Data Breach inflicted significant financial damage upon the Plaintiff and the class, who must act immediately to mitigate potentially present fraud, while simultaneously taking steps to prevent future fraud and while continuing to meet the demands and needs of their financial lives.

55. The costs suffered by the Plaintiff and the class as a result of StockX's data breach, measured in dollars as well as anxiety, emotional distress, and loss of privacy, will continue to mount.

COUNT ONE
VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681, *et seq*.
(On Behalf of the Nationwide Class)

56. Plaintiff repeats and realleges Paragraphs 1-55 as if fully alleged herein.

57. Each time that StockX opens or potentially opens a new account, it obtains, reviews, and use a "consumer report," as that term is defined in 15 U.S.C § 1681a(d), about the person or entity for whom the account is opened or the service started.

58. StockX is required by 15 U.S.C. §§ 1681b, 1681n, and 1681o to refrain from obtaining, disclosing or using consumer reports under false pretenses, and without proper authorization from the person or entity who is the subject of the report.

59. The furnishing of a consumer report is only permitted in specific instances. 15 U.S.C. §§ 1681b(a). Disclosing, or allowing consumer reports to be disclosed, is not allowed pursuant to FCRA, and thus is a violation of federal law.

60. Once obtained, StockX has a mandatory duty to maintain and protect the use of consumer reports for permissible purposes only. 15 U.S.C. § 1681b(f). That includes instances

where, but for actions taken or not taken by StockX in data protection, the use of unlawful consumer reports obtained would not have occurred.

61. Despite these clear and unambiguous requirements of the FCRA, StockX's actions and inactions has caused and will cause consumer reports regarding consumers to be obtained without their knowledge or consent in order to potentially open new, unauthorized accounts, in violation of FCRA.

62. Further, reports that were obtained in relation to the accounts were part of the collection of data that was exfiltrated in the data breach. Accordingly, StockX failed to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

63. StockX failed to maintain reasonable procedures designed to limit the furnishing of class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of class members' consumer reports to unauthorized entities or hackers.

64. As a direct and proximate result of StockX's actions and failures to act described herein, and utter failure to take adequate and reasonable measures to ensure its data systems were protected, StockX offered, provided, and furnished Plaintiff's and class members' consumer reports to unauthorized third parties.

65. Pursuant to 15 U.S.C. §§ 1681n and 1681o, StockX is liable for negligently and willfully violating FCRA by accessing the consumer reports without a permissible purpose or authorization under FCRA.

COUNT TWO
NEGLIGENCE
(On Behalf of the Nationwide Class)

66. Plaintiff repeats and realleges Paragraphs 1-65 as if fully alleged herein.

67. StockX owed a duty to the Plaintiff and the class to use and exercise reasonable and due care in obtaining, retaining, securing, and deleting the Private Information of customers.

68. StockX owed a duty to Plaintiffs and the class to provide security, at a minimum consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Private Information of customers.

69. StockX owed a duty of care to the Plaintiff and the class because they were a foreseeable and probable victim of any inadequate data security practices. StockX solicited, gathered, and stored the sensitive data provided by the Plaintiff and the class. StockX knew it inadequately safeguarded this information on its computer systems and that hackers would attempt to access this valuable data without authorization. StockX knew that a breach of its systems would inflict damages upon the class, and StockX was therefore charged with a duty to adequately protect this critically sensitive information.

70. StockX maintained a special relationship with the class. The class entrusted StockX with Private Information on the premise that it would safeguard this information, and StockX was in a position to protect against the harm suffered by the class as a result of the Data Breach.

71. In light of its special relationship, StockX knew, or should have known, of the risks inherent in collecting and storing the Private Information and the importance of providing adequate security of that information.

72. StockX's own conduct also created a foreseeable risk of harm. Its misconduct included, but was not limited to, it not following broadly accepted security practices and not complying with industry standards for the safekeeping and maintenance of Private Information.

73. StockX breached the duties it owed by failing to exercise reasonable care and implement adequate security protocols—including protocols required by industry rules—sufficient to protect the Private Information at issue.

74. StockX breached the duties it owed by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

75. StockX breached the duties it owed by failing to properly maintain the sensitive Private Information. Given the risk involved and the amount of data at issue, StockX's breach of its duty was entirely unreasonable.

76. StockX, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and class members the fact that their Private Information within its possession might have been compromised and precisely the type of information compromised.

77. Further, because StockX's ongoing failure to notify consumers regarding what type of information has been compromised, consumers are unable to take the necessary precautions to mitigate their damages by preventing future fraud.

78. StockX also knew that the Plaintiff and the class were foreseeable victims of a data breach of its systems because of specific laws, regulations, and guidelines requiring it to reasonably safeguard sensitive information or be held liable in the event of a data breach.

79. As a direct and proximate result of StockX's negligent conduct, the Plaintiff and the class has suffered injury and are entitled to damages in an amount to be proven at trial.

80. In failing to secure Plaintiff's and class members' Private Information and promptly and specifically notifying them of the Data Breach, StockX is guilty of oppression, fraud, or malice in that it acted or failed to act with a willful and conscious disregard of Plaintiff's and class members' rights. In addition to seeking actual damages, Plaintiff seeks punitive damages on behalf of himself and the class.

81. Plaintiff also seeks injunctive relief on behalf of the class compelling StockX to implement appropriate data safeguarding methods and provide detailed and specific disclosure of what types of information has been compromised.

COUNT THREE
NEGLIGENT MISREPRESENTATION
(On Behalf of the Nationwide Class)

82. Plaintiff repeats and realleges Paragraphs 1-81 as if fully alleged herein.

83. Through its privacy policies and other actions and representations, StockX misrepresented to the Plaintiff and the class that it possessed and maintained adequate data security measures and systems that were sufficient to protect Private Information.

84. StockX further misrepresented that it would secure and protect Private Information by agreeing to comply with both Card Operating Regulations and the PCI DSS.

85. StockX knew or should have known that it was not in compliance with the representations made in its privacy policies and the requirements of Card Operating Regulations and the PCI DSS.

86. StockX knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to the Plaintiff and the class.

87. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to the Plaintiff and the class.

88. StockX also failed to exercise reasonable care when it failed to timely communicate information concerning the Data Breach that it knew, or should have known, compromised the Private Information of customers.

89. Further, StockX failed to adequately, timely and specifically communicate the occurrence of the Data Breach in a way that could inform and protect customers.

90. Plaintiff and the class relied upon these misrepresentations and omissions to their detriment.

91. As a direct and proximate result of StockX's negligent misrepresentations and omissions, Plaintiff and the class have suffered and will continue to suffer injury and are entitled to damages in an amount to be proven at trial.

COUNT FOUR
VIOLATION OF MICHIGAN IDENTITY THEFT STATUTE
(On Behalf of the Nationwide Class)

92. Plaintiff repeats and realleges Paragraphs 1-91 as if fully alleged herein.

93. StockX owns, licenses and/or maintains computerized data that includes Plaintiff's and class members' Private Information. StockX failed to take all reasonable steps to protect or make unreadable or undecipherable records within its custody or control.

94. The Data Breach constituted a "security breach" that required specific notice within the meaning of the Identity Theft Protection Act. Mich. Comp. Laws Ann. § 445.72 (2006). StockX violated the Act by unreasonably delaying disclosure of the Data Breach to consumers whose Private Information was exposed.

95. Upon information and belief, no state or federal law enforcement agency instructed StockX that notification to Plaintiff or the class would impede a criminal investigation.

96. As a result of StockX's violation of the Identity Theft Protection Act, users incurred economic damages, including expenses associated with monitoring their Private Information to prevent fraud.

97. Plaintiff seeks all remedies available under the Identity Theft Protection Act. Because StockX was guilty of oppression, fraud or malice, in that it failed to act with a willful and conscious disregard of users' rights, Plaintiff also seeks punitive damages.

COUNT FIVE
INTRUSION UPON SECLUSION
(On Behalf of the State Subclass)

98. Plaintiff repeats and realleges Paragraphs 1-97 as if fully alleged herein.

99. Plaintiff had a reasonable expectation of privacy in the Private Information that StockX failed to protect. Pennsylvania recognizes that expectation as a right.

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1976).

100. In failing to protect Plaintiff's data, StockX allowed for or invaded Plaintiff's and the class' privacy by intruding into Plaintiff's private affairs in a manner that would be highly offensive to a reasonable person and by publicizing private facts about the Plaintiffs, which is highly offensive to a reasonable person.

101. StockX knew or acted with reckless disregard of the fact that a reasonable person in Plaintiff's position would consider StockX's actions highly offensive.

102. StockX invaded Plaintiff's right to privacy and intruded into his private affairs by misusing and/or disclosing Private Information without informed, voluntary, affirmative, and clear consent, amounting to a serious invasion of Plaintiff's protected privacy interests.

103. As a proximate result of such misuse and disclosures, Plaintiff's reasonable expectation of privacy in his Private Information was unduly frustrated and thwarted.

104. In failing to protect Plaintiff's Private Information, and in misusing and/or disclosing his Private Information, StockX acted with malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of himself and the class.

COUNT SIX
VIOLATIONS OF PENNSYLVANIA'S UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
(On Behalf of the State Subclass)

105. Plaintiff repeats and realleges Paragraphs 1-104 as if fully alleged herein.

106. This claim is asserted on behalf of the members of the State Subclass under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), PA ST 73 P.S. § 201-1, *et seq.*

107. StockX's collection of Private Information constitutes unfair and/or deceptive acts or practices in violation of the UTPCPL, PA ST 73 P.S. §201-1, *et seq.*

108. The UTPCPL, PA ST 73 P.S. § 201-3 prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

109. PA ST 73 P.S. § 201-2(4)(xxi) defines "unfair methods of competition" and "unfair or deceptive acts or practices" as "engaging in any other fraudulent tor deceptive conduct which creates a likelihood of confusion or misunderstanding."

110. Pursuant to PA ST 73 P.S. § 201-9.2, *et seq.*, Plaintiff and members of the State Subclass maintained accounts with StockX that were used primarily for personal, family or household purposes.

111. StockX engaged in unlawful conduct, made affirmative misrepresentations, or otherwise violated the UTPCPL by, *inter alia*, knowingly and intentionally collecting and failing to adequately protect Private Information, and misrepresenting and failing to disclose its inadequate policy and practice of protecting Private Information.

112. StockX also engaged in unlawful conduct in violation of the UTPCPL by making knowing and intentional omissions. StockX knowingly failed to disclose the true nature of its data security policy and practice, and failed to adequately disclose the scope, nature and details of the Data Breach in violation of law.

113. StockX intended that Plaintiff and all class members rely on the acts of concealment and omissions, so that Plaintiff and all class members would feel secure providing StockX their valuable Private Information.

114. StockX's conduct caused Plaintiff and class members to suffer actual, ascertainable losses that, but for StockX's unfair and deceptive policy, would not otherwise have been incurred.

115. A causal relationship exists between StockX's unlawful conduct and the ascertainable losses suffered by Plaintiff and the class. Had StockX adequately protected the Private Information at issue here, Plaintiff and the class would not have incurred losses in violation of the UTPCPL.

116. As redress for StockX's repeated and ongoing violations of the UTPCPL, Plaintiff and the State subclass are entitled to, *inter alia*, damages and declaratory relief declaring StockX's practices to be unlawful, unfair, unconscionable and/or deceptive, and enjoining StockX from undertaking any further unlawful, unfair, unconscionable, and/or deceptive acts or omissions.

117. Because Plaintiff seeks to enforce an important right affecting the public interest, Plaintiff requests an award of attorneys' fees and costs on behalf of himself and the class.

COUNT SEVEN
DECLARATORY RELIEF
(On Behalf of the Nationwide Class and the State Subclass)

118. Plaintiff repeats and realleges Paragraphs 1-117 as if fully alleged herein.

119. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

120. An actual controversy has arisen in the wake of the StockX Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether StockX is currently maintaining data security measures adequate to protect Plaintiff and class members from further data breaches that compromise their Private Information. Plaintiff allege that StockX's data security measures remain inadequate. StockX denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and remains at imminent risk that further compromises of Private Information will occur in the future.

121. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. StockX continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. StockX continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

122. The Court also should issue corresponding prospective injunctive relief requiring StockX to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information and to adequately disclose information regarding the Data Breach.

123. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at StockX. The risk of another such breach is real, immediate, and substantial. If another breach at StockX occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

124. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to StockX if an injunction is issued. Among other things, if another massive data breach occurs at StockX, Plaintiff will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to StockX of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and StockX has a pre-existing legal obligation to employ such measures.

125. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at StockX, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of himself and the class, respectfully requests that the Court enter judgment in their favor as follows:

a. certifying the class under Fed. R. Civ. P. 23 and appointing Plaintiff and its counsel to represent the class pursuant to Fed. R. Civ. P. 23(g);

b. awarding Plaintiff and the class monetary damages as allowable by law;

c. awarding Plaintiff and the class appropriate equitable relief;

d. awarding Plaintiff and the class pre-judgment and post judgment interest;

e. awarding Plaintiff and the class reasonable attorneys' fees and costs as allowable by law; and

f. awarding all such further relief as allowable by law.

JURY TRIAL DEMANDED

Plaintiff, on behalf of himself and the class, demands a trial by jury on all issues so triable.

Richard M. Golomb, Esquire
Kenneth J. Grunfeld, Esquire
GOLOMB & HONIK, P.C.
1835 Market Street, Suite 2900
Philadelphia, PA 19103
Phone: (215) 985-9177
Fax: (215) 985-4169

Attorneys for Plaintiff and the Class

Dated: August 15, 2019